

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Lenovo ThinkPad laptop, serial number PC-05F685  
15/06, currently located at the Federal Bureau of  
Investigation, 7747 Clys Road, Centerville, OH, 45459

Case No.

3:19 mj 401

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment Alocated in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

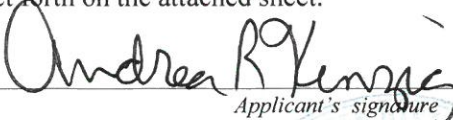
Code Section

See Attachment C

Offense Description

The application is based on these facts:  
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 7-18-19



Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

**ATTACHMENT A**

**DESCRIPTION OF PROPERTY TO BE SEARCHED**

The property to be searched is a Lenovo ThinkPad laptop, serial number PC-05F685 15/06 (hereinafter referred to as "SUBJECT DEVICE"). The SUBJECT DEVICE is currently located at the Federal Bureau of Investigation, 7747 Clys Road, Centerville, Ohio, 45459.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED AND SEARCHED**

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession and attempted of child pornography); and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography.
2. Any visual depictions of minors.
3. Any Internet history indicative of searching for child pornography.
4. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.
6. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
7. Lists of computer and Internet accounts, including user names and passwords.
8. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the iCloud account.
9. Any information related to the use of aliases.
10. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

**ATTACHMENT C**

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography



**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

**INTRODUCTION**

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — an electronic device — which is currently in law enforcement’s possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
3. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child exploitation offenses committed by CHARLEY DUNHAM JR. (hereinafter referred to as “DUNHAM”). As further detailed below, the investigation has determined that DUNHAM has utilized the account names of “kt13631”, “katie13631”, and “tykmiller” on a smartphone instant messenger application; namely, the Kik Messenger application. This Affidavit is submitted in support of an Application for a search warrant for the following:
  - a. Lenovo ThinkPad laptop, serial number PC-05F685 15/06, currently located at the Federal Bureau of Investigation, 7747 Cloyo Road, Centerville, Ohio, 45459 (hereinafter referred to as the “**SUBJECT DEVICE**”).
4. The purpose of the Application is to seize evidence of the following violations:
  - a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography; and
  - b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce.

5. The items to be searched for and seized are described more particularly in Attachment B hereto and are incorporated by reference.
6. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
7. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the search of the **SUBJECT DEVICE**.
8. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present within the information located on **SUBJECT DEVICE**.

#### **PERTINENT FEDERAL CRIMINAL STATUTES**

9. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
10. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
11. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or



affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

12. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

### **BACKGROUND INFORMATION**

#### **Definitions**

13. The following definitions apply to this Affidavit and Attachment B to this Affidavit:
  - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
  - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
  - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
  - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

- e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. A network **“server,”** also referred to as a **“host,”** is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A **“client”** is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook



or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

- i. **“Domain Name”** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and, “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.
- j. **“Log Files”** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- m. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a



common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

- n. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### Collectors of Child Pornography

- 14. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):
  - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
  - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

#### Kik Messenger Application

- 15. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.
- 16. The Kik messenger application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.
- 17. Unlike many other smartphone instant messenger applications that are based on a user’s telephone number, Kik uses usernames to identify its users. Each user selects and is



assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. Kik Interactive Inc. does not verify this information, and as such, users can provide inaccurate information.

18. Kik Interactive Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, Kik Interactive Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. Kik Interactive Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). Kik Interactive Inc. does not store or maintain chat message content.
19. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.

#### IMGSRC.RU Website

20. IMGSRC.RU is a Russian image board website that allows users to upload photos and post comments to their own photos and the photos of other users. Users are able to create account profiles, although a profile does not need to be maintained in order to browse photos posted by others. Based on my training and experience, I know that the IMGSRC.RU image board is a popular means for storing and trading child pornography and posting comments about the sexual exploitation of children.

#### Use of Computers and the Internet with Child Pornography

21. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.
  - a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed

directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.

- b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.
- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.
- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of



these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

### **FACTS SUPPORTING PROBABLE CAUSE**

#### **Initial Investigation**

22. In 2017 and 2018, agents and investigators from the Kansas City, Missouri division of the FBI investigated STEVEN DEAN FRENCH (hereinafter referred to as "FRENCH") for child pornography and child exploitation offenses. On or around August 29, 2018, a federal search warrant was executed at FRENCH's residence in Columbia, Missouri. Various electronic media were seized pursuant to the search warrant.
23. During the execution of the search warrant, FRENCH agreed to be interviewed. FRENCH admitted that he viewed child pornography files, and that he had traded child pornography files with his online acquaintances. FRENCH also admitted that he sometimes role-played with his online acquaintances, including role-playing about having sex with children. During these role-playing activities, either FRENCH or the person with whom he was communicating sometimes posed as a child.
24. The electronic media seized from FRENCH's residence were examined pursuant to the search warrant, and child pornography files were recovered from one or more devices. On or around September 19, 2018, FRENCH was indicted for one count of possession of child pornography (in violation of 18 U.S.C. § 2252(a)(2)) and one count of receipt of child pornography (in violation of 18 U.S.C. § 2252(a)(4)(B)).
25. Data recovered from FRENCH's electronic devices revealed that he utilized a Kik account to receive child pornography files from others. One of the Kik users whom FRENCH communicated with and received child pornography files from was an individual who utilized the Kik account name of "kt13631" and a profile name of "KATIE TYSON". Below is a summary of messages exchanged between FRENCH and "KATIE TYSON" during the approximate time period of August 22, 2017 through March 17, 2018:
  - a. The conversation began with FRENCH saying that he had seen albums that depicted "KATIE TYSON" and her "girls" on the IMGSRU website.
  - b. "KATIE TYSON" indicated that she had three juvenile daughters. "KATIE TYSON" made numerous comments indicating that she fantasized about



watching others engage in sexual activities with her daughters. By way of example, below are excerpts of some of “KATIE TYSON’s” comments from on or around January 1, 2018:

KATIE TYSON: Basically I would let anything be done to them. It’s never happened but I think and fantasize about it all the time

FRENCH: Mmmm...that would be very open minded! Is there a particular one of the three that you fantasize about?

KATIE TYSON: I think I fantasize about my youngest the most but I guess it just depends on my mood

.....

FRENCH: Would you like seeing that young vagina be made to stretch open enough to accept a man inside her?

KATIE TYSON: Hell yes! Lol

FRENCH: We would both be on the same page! You may have to help hold her down!

KATIE TYSON: Oh I would definitely love to hold her lil body down. Wouldn’t mind watching her squirm a little

FRENCH: That would make it even hotter! In the end she needs to know that it would only be the first of many times

FRENCH: Would we stop with her, teach her until she could be shared with others who like your pics or would we work on another?

KATIE TYSON: Get her ready to be shared and then move on to the next one and do the same

- c. Later in the conversation, “KATIE TYSON” indicated that she recently allowed another man to engage in sexual activities with one of her daughters. “KATIE TYSON” told FRENCH about several of these purported instances. By way of example, below are excerpts from a conversation on or around March 10, 2018:

FRENCH: Thanks for sharing the pics! How did the little one do last Sunday? Cannot tell you how many times I have thought about you two and that night!

KATIE TYSON: She did great. It was lots of fun *[emoticon]*

FRENCH: Was she able to take him again? Like you hoped she would?

KATIE TYSON: Yes she was.

FRENCH: Is she no longer a little virgin Katie?

KATIE TYSON: No she is definitely not

FRENCH: Oh damn!!! She is going to need it more and soon.  
Have to help keep her used to taking a cock  
KATIE TYSON: Well he couldn't get away and get a hotel so I ended up driving to his house. When we got there I knocked on the door, he opened it and he was standing there nude with a full on erection. I loved it! We ended up going in his computer room and he sat in his chair and I got on my knees and sucked on him as she watched us. Then he watched me undress her as he jerked off and lubed up. I rubbed some on her pussy while kissing on her then he picked her up and sat her on his lap. He fucked her reverse cowgirl so I could sit and watch her reaction. She took 3/4ths of his cock which amazed me for her first time. He fucked her like that for about 10 minutes and when he pulled it out of her to cum he was already squirting cum so I know he was cumming inside of her before he pulled it out. He finished cumming on her body. He is definitely going to get more opportunities after that.

.....

KATIE TYSON: I think she enjoyed it over all. There was a point when she got a bit squirmish when he was really pumping it in her but at that point there was no stopping it

- d. During the approximate time period of January 19, 2018 through March 11, 2018, "KATIE TYSON" sent FRENCH approximately fifty-three image files and one video file, most of which depicted female children. "KATIE TYSON" indicated that her daughters were depicted in these image and video files. The image and video files included the following:
  - i. Approximately twenty of the images and one of the videos depict what appears to be pre-pubescent female children engaged in sexually explicit conduct. Based on my training and experience, I believe that these image and video files depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, four of the files are described as follows:
    - 1. 9400698c-759b-446e-a345-8de7b3080148.jpg: The file is an image that depicts what appears to be a pre-pubescent white female child. The child is holding what appears to be a white male's penis in both of her hands.

2. [b4349e11-a53d-4ef0-95e2-2c8aabe92f95.jpg](#): The file is an image that depicts the nude vagina of what appears to be a pre-pubescent white female child. What appears to be a white male's penis is inserted into the child's vagina.
  3. [ade366c2-3624-4fbb-9069-07d90143e345.jpg](#): The file is an image that depicts what appears to be a pre-pubescent white female child lying on her side. What appears to be a white male's penis is partially inserted into the child's anus.
  4. [8d5b6bac-c5df-4ea9-8558-a579c0d5218d.mp4](#): The file is a video that depicts what appears to be a pre-pubescent white female child lying on her back. The child is wearing a shirt that is pulled up around her chest, and she is nude from the waist down. What appears to be an adult white male masturbates his penis and then engages in vaginal sexual intercourse with the child. Next, the adult male uses his fingers to spread apart the child's vagina. Finally, the adult male uses a tissue or cloth to wipe off what appears to be semen from the child's vagina. The video is approximately one minute and thirty seconds in duration.
- ii. Approximately five of the images depict what appears to be the nude buttocks of a female child.
  - iii. Approximately three of the images depict a close-up of the crotch of what appears to be a female child wearing underwear.
  - iv. Approximately twenty-one of the images depict three female children (either together or separate) wearing clothing in various settings.
26. Based on the comments made by FRENCH at the beginning of his conversation with "KATIE TYSON" (as detailed above), it appears that "KATIE TYSON" had an account on the IMGSRU.RU website. I searched the publicly available content of the IMGSRU.RU website and located an account in the name of "KATIE13631". The publicly available information for the "KATIE13631" account included the following:
- a. The account profile identified that the account was associated with the email address [katie13631@gmail.com](mailto:katie13631@gmail.com), and that the user had joined the website on or around March 12, 2016. The following information was listed in the "user information" for the account: "KIK me at katie13631 – Blonde mom of three blonde girls".



- b. The account contained one album that depicted approximately thirteen images. The images primarily depicted an adult female and three female children. These female children appear to be the same as those depicted in the twenty-one images of female children wearing clothing that were sent from “KATIE TYSON” to FRENCH (as detailed in paragraph 25(d)(iv)).
- 27. Based on the information contained on the IMGSRU website, it appears that the user of the “KATIE13631” IMGSRU account is also the user of the “KATIE TYSON” Kik account. It also appears that the “KATIE TYSON” Kik account user has a second Kik account – that being an account with an account name of “katie13631”.

Subpoenaed Records and Other Information

- 28. On or around December 18, 2018, an FBI agent served a subpoena to Kik Interactive Inc. requesting subscriber information for the Kik account name of “kt13631” (the account utilized to communicate with FRENCH), as well as logs of IP addresses utilized to access the account and transmit messages. Records provided by Kik Interactive Inc. in response to the subpoena provided the following information:
  - a. A Kik account with an account name of “kt13631” and a profile name of “KATIE TYSON” was created on or around February 2, 2015. The email address [kt13631@gmail.com](mailto:kt13631@gmail.com) was associated with the account profile.
  - b. As of the date of the subpoena, the “KATIE TYSON” account user had not accessed the Kik account since on or around May 29, 2018. The IP address of 98.29.144.231 was utilized to access the account on this date.
  - c. Kik Interactive Inc.’s records identified that an iPhone was used to access the account on or around December 21, 2017.
- 29. On or around February 22, 2019, an FBI agent served a subpoena to Kik Interactive Inc. requesting subscriber information for the Kik account name of “katie13631” (the account listed on the “KATIE13631” IMGSRU account), as well as logs of IP addresses utilized to access the account and transmit messages. Records provided by Kik Interactive Inc. in response to the subpoena provided the following information:
  - a. A Kik account with an account name of “katie13631” and a profile name of “KATIE MILLER” was created on or around June 6, 2018. The email address [katie13631@gmail.com](mailto:katie13631@gmail.com) was associated with the account profile.
  - b. As of the date of the subpoena, the “KATIE MILLER” account user had not accessed the Kik account since on or around January 12, 2019. The IP address of 98.30.221.170 was utilized to access the account on this date.

- c. Kik Interactive Inc.'s records identified that an iPhone was used to access the account on or around June 6, 2018.
30. Charter Communications was identified as the service provider for the IP address 98.29.144.231 (the IP address utilized to access the "kt13631" Kik account). On or around December 19, 2018, an administrative subpoena was served to Charter Communications requesting subscriber information for this IP address on May 29, 2018, at the approximate time it was used to access the "KATIE TYSON" Kik account. Records received in response to the subpoena identified that the IP address was subscribed to DUNHAM at 107 Pearl Street, New Paris, Ohio (hereinafter referred to as the "SUBJECT PREMISES"). The Records identified that DUNHAM's telephone number was 937-336-8131, and that his Internet account was activated on or around April 22, 2016.
31. Charter Communications was also identified as the service provider for the IP address 98.30.221.170 (the IP address utilized to access the "katie13631" Kik account). On or around February 26, 2019, an administrative subpoena was served to Charter Communications requesting subscriber information for this IP address on January 12, 2019, at the approximate time it was used to access the "katie13631" Kik account. Records received in response to the subpoena identified that the IP address was subscribed to DUNHAM at the SUBJECT PREMISES. The records again identified that DUNHAM's telephone number was 937-336-8131.
32. Based on records from the Ohio Bureau of Motor Vehicles, DUNHAM utilizes the SUBJECT PREMISES on his current Ohio driver's license. This driver's license was issued on or around October 5, 2018.
33. AT&T was identified as the service provider for telephone number 937-336-8131 (the number reflected in Charter Communications' records as being DUNHAM's telephone number). On or around January 16, 2019, an FBI investigator served AT&T with a subpoena requesting subscriber information for this telephone number, including the make and model number of the device utilizing the telephone number. Records received in response to the subpoena identified that the telephone number was subscribed to DUNHAM at an address in Richmond, Indiana. Records also identified that an Apple iPhone bearing model number XA1901 utilized this telephone number. As detailed above, an iPhone had accessed the "kt13631" and "katie13631" Kik accounts.
34. On or around December 27, 2018, an FBI agent served Google LLC with a subpoena requesting subscriber information for the email address [kt13631@gmail.com](mailto:kt13631@gmail.com) (the email address utilized to register the kt13631 Kik account). Records received from Google LLC in response to the subpoena identified that the account was created on or around July 16, 2014, in the name of "ALEX TYSON".



35. As part of the investigation, a number of the child pornography images that “KATIE TYSON” sent to FRENCH that purportedly depicted her daughters were sent to the National Center for Missing and Exploited Children (NCMEC) for comparison to the Child Victim Identification Program (CVIP) database. The CVIP database maintains child pornography files that have been recovered from law enforcement agencies worldwide. Through this database, NCMEC analysts maintain information about children depicted in the files who have already been identified by law enforcement officers, and they are able to identify when these files are recovered in other investigations. A NCMEC analyst determined that at least approximately six of the image files sent by “KATIE TYSON” to FRENCH represented two known series (i.e., files depicting children who have been previously identified by other law enforcement agencies). As such, it does not appear that these images depict “KATIE TYSON’s” daughters, as she purported them to be.
36. Utilizing various investigative tools, an FBI investigator located a Facebook account for a woman residing in Xenia, Ohio who will be referred to for purposes of this Affidavit as “Adult Female A”. Photographs of three female children were posted on the publicly available content of Adult Female A’s Facebook account. These children appeared to be the same as those depicted in the twenty-one images of female children wearing clothing that were sent from “KATIE TYSON” to FRENCH (as described in paragraph 25(d)(iv)). Adult Female A and the three children depicted on her Facebook page also appear to be the same individuals as those depicted on the “KATIE13631” IMGSRU.RU account (as described in paragraph 26(b)).
37. Based on my training and experience, I know that individuals involved in child exploitation offenses often utilize one or more aliases as a means to avoid detection from law enforcement officers. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Also based on my training and experience, I know that individuals involved in child exploitation offenses sometimes role-play about their sexual fantasies, and they utilize multiple identities (to include different ages and genders) as part of this role-playing. As detailed above, FRENCH reported that he sometimes role-played with his online acquaintances. Based on all of the information detailed in the Affidavit, it appears that “KATIE TYSON” may be using a false identity.
38. Also based on my training and experience, I know that individuals involved in child exploitation offenses sometimes search social media applications and other Internet websites for pictures of children who they find attractive. These offenders often use these pictures for their sexual fantasies, sexual gratification, and role-playing activities. I have been involved in other investigations in which offenders have falsely identified that children depicted in photographs were their children or relatives. Again based on all of the information detailed in the Affidavit, it appears that “KATIE TYSON” may be falsely

identifying children depicted in various image and video files to be his/her daughters.

Execution of Search Warrant

39. On or around February 20, 2019, agents and task force officers of the FBI searched the SUBJECT PREMISES pursuant to a search warrant authorized by the United States District Court for the Southern District of Ohio. DUNHAM was the only individual present when agents and officers arrived to execute the warrant. A desktop computer and an iPhone (the same make of cellular telephone that was utilized to access the “kt13631” and “katie13631” Kik accounts) were located and seized pursuant to the warrant.
40. During the execution of the search warrant, DUNHAM agreed to be interviewed after being advised of his Miranda rights. Below is a summary of some of the information provided by DUNHAM during the interview:
  - a. DUNHAM resided alone at the SUBJECT PREMISES.
  - b. DUNHAM had an iPhone bearing telephone number 937-336-8131. He also had a desktop computer in his residence. DUNHAM was the only individual who utilized these devices.
  - c. DUNHAM received Internet service through Spectrum (which is owned by Charter Communications). A password was required to access DUNHAM’s Internet account, and DUNHAM was the only individual who utilized the Internet service.
  - d. DUNHAM previously utilized Kik accounts in the names of “kt13631” and “katie13631”. He utilized either the email address [kt13631@gmail.com](mailto:kt13631@gmail.com) or [katie13631@gmail.com](mailto:katie13631@gmail.com) to register the “kt13631” Kik account (but he did not identify which email address he utilized to register the “katie13631” Kik account). DUNHAM first utilized the “kt13631” account, but Kik closed this account. DUNHAM thereafter opened the “katie13631” account. Within the past month, DUNHAM opened another Kik account in a name that he could not recall. DUNHAM utilized the email address [kt13631@yahoo.com](mailto:kt13631@yahoo.com) to register this Kik account.
  - e. When communicating with others on Kik Messenger, DUNHAM had sent and received images and videos depicting children who were approximately three to eighteen years old and who were nude and/or engaged in sexual activities. DUNHAM traded these types of files a few times per week. DUNHAM estimated that he began trading child pornography files approximately two to three years ago. DUNHAM saved the child pornography files on his iPhone and



in his Mega cloud storage account<sup>1</sup>. DUNHAM estimated that he had viewed hundreds of images and approximately 20 videos of child pornography.

- f. DUNHAM had an account on the IMGSRU website in the name of “katie13631”. He primarily met his child pornography trading partners on the IMGSRU website.
  - g. DUNHAM acknowledged that he knew Adult Female A’s family, and that he had met them through one of his family members. DUNHAM was shown a photograph of Adult Female A and her family members, and he was able to identify all of them by name. DUNHAM stated that he had met Adult Female A’s children on one occasion, but that he was never alone with them.
  - h. DUNHAM admitted that he had used pictures of Adult Female A’s children when he communicated with others on Kik Messenger. He used the pictures so that he and the people who he was communicating with could make sexual comments about them. In the communications, DUNHAM had posed as Adult Female A and the mother of her children. DUNHAM had role played about one of the children having sex with men.
  - i. DUNHAM had obtained pictures of Adult Female A’s children from her Facebook account. DUNHAM was friends with Adult Female A on Facebook, but they did not communicate with each other.
  - j. DUNHAM was shown screen prints of the “katie13631” account on the IMGSRU website. DUNHAM confirmed that this was his account and that the pictures on the account depicted Adult Female A and her children. DUNHAM was also shown some of the messages that were exchanged between FRENCH and the “kt13631” Kik account. DUNHAM acknowledged that the communications appeared to be his.
  - k. DUNHAM utilized the email address [charleydunham@gmail.com](mailto:charleydunham@gmail.com). He utilized the [kt13631@gmail.com](mailto:kt13631@gmail.com), [katie13631@gmail.com](mailto:katie13631@gmail.com), and [kt13631@yahoo.com](mailto:kt13631@yahoo.com) email addresses to register his Kik accounts. He also utilized the email address [kt13631@gmail.com](mailto:kt13631@gmail.com) to log into his Mega account.
41. Pursuant to the search warrant, an examination has been conducted of the iPhone that was seized from DUNHAM’s residence. Below is a summary of information obtained during the preliminary examination:

---

<sup>1</sup> Mega is a cloud storage and file hosting service that allows users to store their files on Mega’s servers. The service is offered by Mega Limited, a company based in New Zealand. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded to Mega’s servers, preventing others from accessing the files. Based on my training and experience, I know that individuals involved in child pornography offenses often use cloud storage services such as Mega to store and conceal their files.

- a. The device was an iPhone 10. The owner name of the device was "CHARLEY DUNHAM", and the device's telephone number was 937-336-8131 (the telephone number DUNHAM identified as being his number and that is subscribed to him).
- b. A number of images were recovered from the telephone depicting children in various states of undress, including images depicting sexually explicit conduct. Based on my training and experience, it appears that more than 2,200 of the images and more than 70 of the videos depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, five of the files depicting child pornography are described as follows:
  - i. !!!New!!! (Pthc) Nina 2 (7Yo Bj) AND 7yo\_suck\_2.mp4: The file is a video that depicts what appears to be a nude pre-pubescent white female child lying on a bed. What appears to an adult white male inserts his penis into the child's mouth. The video is approximately two minutes and twelve seconds in duration.
  - ii. 00000 s\_per 11 yo fuck 433H.mp4: The file is a video that depicts what appears to be a pre-pubescent white female child who is wearing a shirt but is nude from the waist down. The child inserts her fingers into her vagina. What appears to be an adult white male then has vaginal sexual intercourse with the child. The video is approximately two minutes and forty-four seconds in duration.
  - iii. 074-nude.jpg: The file is an image that depicts what appears to be a white female child lying on a bed. The child is wearing a shirt that is pulled up around her chest, and she is nude from the waist down. What appears to be a penis is inserted into the child's vagina.
  - iv. 031-nude.jpg: The file is a close-up image that depicts what appears to be the nude vagina and anus of a pre-pubescent white female child. What appears to be a penis is inserted into the child's anus.
  - v. 142495170482.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white female child lying on the floor with her legs spread apart, exposing her nude vagina to the camera. The child's wrists and ankles are bound to the floor with a black material, and there is a material covering her eyes.
- c. A Kik account was established on the telephone. The account name for this Kik account was "tykmiller" (which includes Adult Female A's nickname and last name). The email address associated with this Kik account was



[tykmiller13@yahoo.com](mailto:tykmiller13@yahoo.com). The “tykmiller” Kik account exchanged messages with approximately four other account users. Below is a summary of these messages:

- i. On or around February 11, 2019, the “tykmiller” account received a message that appeared to be from Kik Interactive Inc. This message indicated that the “tykmiller” account was opened on or around February 11, 2019.
- ii. Consistent with the information provided by DUNHAM during the interview, the “tykmiller” account user told two of the other users that Kik had recently closed his previous Kik account. The “tykmiller” account user told one of the other Kik users that if his Kik account was closed again, the other user could email him.
- iii. The “tykmiller” account user sent photographs of Adult Female A and her children to two other Kik users. The “tykmiller” account user and the individuals who he communicated with made sexually explicit comments about Adult Female A’s children.
- iv. A number of images and videos of children were exchanged between the “tykmiller” account user and two other Kik users. Based on my training and experience, I believe that the “tykmiller” account user received one video file depicting child pornography (as defined by 18 U.S.C. § 2256(8)) from another Kik user on or around February 13, 2019. This video is described as follows:
  1. 63960165-73bd-8059-e20162074cc5: The file is a video that depicts what appears to be an adult white male inserting his penis into the mouth of what appears to be a pre-pubescent white female child. The child is crying throughout the video. The video is approximately one minute and thirty seconds in duration.
- d. Adult Female A’s Facebook account name was listed in the contact list for the iPhone. Pictures of Adult Female A and her children were recovered from the device.
- e. The web history for the device indicated that the user accessed URL’s associated with the IMGSRU website on approximately 1,841 occasions, as recently as on or around February 16, 2019. Based on the titles of these websites, it appeared that a number of them contained content involving children. By way of example, on or around February 14, 2019, the user accessed a URL with the following title: “Panties my niece 8 years old, Myniece 7 yo panties 25@ iMGSRU”.



- f. The Internet search history for the device identified that the user conducted a number of searches on or around September 29, 2018. Based on my training and experience, the user's search terms are consistent with someone searching for child exploitation materials. These search terms included the following: "child prostitution", "child trafficking erotica", "child trafficking", "black child model", "thai child model", "thai child swimsuit model", "korean child swimsuit model", "korean child model", "asian child model", and "child swimwear model".
  - g. Cached Gmail accounts associated with [charleydunham@gmail.com](mailto:charleydunham@gmail.com), [katie13631@gmail.com](mailto:katie13631@gmail.com), and [kt13631@gmail.com](mailto:kt13631@gmail.com) were established on the iPhone.
42. Also pursuant to the search warrant, an examination has been conducted of the desktop computer that was seized from DUNHAM's residence. Below is a summary of information obtained during the preliminary examination:
- a. A number of images were recovered from the computer depicting children in various states of undress, including images depicting sexually explicit conduct. Based on my training and experience, it appears that more than 125 of the images depict child pornography (as defined by 18 U.S.C. § 2256(8)). All of the files were recovered from the deleted space of the computer, and as such, the file names and file dates were not available. By way of example, three of the files depicting child pornography are described as follows:
    - i. File 1: The file is an image that depicts the abdomen, vagina, and upper thighs of what appears to be a nude pre-pubescent white female child. A white rope is tied around the child's waist and legs. What appears to be the fingers of a white male are inserted into the child's vagina.
    - ii. File 2: The file is an image that depicts what appears to be a pre-pubescent white female child performing fellatio on the penis of what appears to be an adult white male. The adult white male is holding the child's mouth open.
    - iii. File 3: The file is a close-up image of the nude vagina and anus of what appears to be a pre-pubescent white female child. What appears to be a penis is inserted into the child's anus.
  - b. More than 60 images of Adult Female A and her children were recovered from the computer.
  - c. An iOS Kik Messenger user account in the name of "kt13631" was recovered from the computer.

- d. Approximately 214 messages from the Kik Messenger application were recovered from the computer. The messages were exchanged during the approximate time period of January 21, 2017 through February 3, 2017. The account name for the owner of these messages was not identified in the records recovered from the computer. However, based on the iOS Kik Messenger user account recovered from the computer (as detailed above in paragraph 42(c)) and other information detailed in the Affidavit, it is reasonable to believe that the “kt13631” account sent and received the messages recovered from the computer. The Kik messages recovered from the computer included the following:
    - i. Images of children were attached to some of the messages, including at least one of Adult Female A’s children.
    - ii. The messages included references to content on the IMGSRU website.
    - iii. The messages included discussions about children engaging in sexual activities.
    - iv. The messages included the exchange of Dropbox sharing links.
  - e. The Dropbox application was installed on the computer. A number of URL’s associated with the Dropbox website were also accessed from the computer.
  - f. URL’s associated with the IMGSRU website were accessed on over one thousand occasions.
43. Based on all of the information detailed above, there is probable cause to believe that DUNHAM is the user of the “kt13631”, “katie13631”, and “tykmiller” Kik accounts as well as the Apple iPhone and desktop computer seized from his residence. There is also probable cause to believe that DUNHAM has utilized these Kik accounts, his iPhone, and his desktop computer to possess, receive, and distribute child pornography files.

Additional Records from Kik Interactive Inc.

44. On or around February 26, 2019, an FBI agent served a subpoena to Kik Interactive Inc. requesting subscriber information for the Kik account name of “tykmiller” (the account recovered from DUNHAM’s iPhone), as well as logs of IP addresses utilized to access the account and transmit messages. Records provided by Kik Interactive Inc. in response to the subpoena provided the following information:
- a. A Kik account with an account name of “tykmiller” and a profile name of “TYK MILLER” was created on or around February 11, 2019. The email address [tykmiller13@yahoo.com](mailto:tykmiller13@yahoo.com) was associated with the account profile.



- b. The logs of IP addresses identified that the “tykmiller” account user had accessed the account on a number of occasions during the approximate time period of February 11, 2019 through February 19, 2019. The IP address of 98.30.221.170 (the same IP address utilized to access the “katie13631” Kik account and that is registered to DUNHAM at the SUBJECT PREMISES) was utilized to access the account on all of the occasions.
- c. Kik Interactive Inc.’s records identified that an iPhone was used to access the account on or around February 11, 2019.

Identification of Adult Female A

45. On or around February 26, 2019, Adult Female A and her husband (hereinafter referred to as “Adult Male B”) were contacted and interviewed. In summary, Adult Female A and Adult Male B provided the following information:
- a. Adult Female A and Adult Male B met DUNHAM through one of DUNHAM’s family members. Their personal interactions with DUNHAM were very limited.
  - b. DUNHAM was on Adult Female A’s friends’ list on Facebook. Adult Female A did not remember personally communicating with DUNHAM on Facebook on any past occasions.
  - c. Adult Female A and Adult Male B had three daughters who were 12 years old, 11 years old, and 8 years old. Adult Female A and Adult Male B were not specifically aware of any occasions when DUNHAM was around their children.
  - d. Adult Female A and Adult Male B were shown a sample of photographs that were sent by the “kt13631” Kik account to FRENCH. Adult Female A and Adult Male B identified that their children were depicted in the photographs. They also identified that these photographs were previously posted on Adult Female A’s Facebook and/or Instagram accounts.
  - e. Adult Female A was shown the profile picture for the “tykmiller” Kik account. Adult Female A advised that she was the individual depicted in the profile picture, but she had no knowledge of the Kik account. Neither Adult Female A nor Adult Male B had ever used the Kik Messenger application.

Collection of Additional Devices

46. On or around March 13, 2019, an arrest warrant was authorized by the United States District Court for the Southern District of Ohio charging DUNHAM with two counts of distribution of child pornography, in violation of 18 U.S.C. §§2252(a)(2) and (b)(1); one count of receipt of child pornography, in violation of 18 U.S.C. §§2252(a)(2) and (b)(1); and one count of possession of child pornography, in violation of 18 U.S.C.

§§2252(a)(4)(B) and (b)(2). DUNHAM surrendered himself to the United States Marshal's Service on or around March 14, 2019. He thereafter was granted a bond and was released on pre-trial release.

47. As part of the conditions of DUNHAM's bond, he was forbidden from possessing and using computer devices that are capable of accessing the Internet and storing data, with the exception of devices that were utilized for employment purposes. DUNHAM informed Pretrial Services that he utilized a computer at his place of employment that was part of some type of computer terminal. DUNHAM did not inform Pretrial Services that he was issued a laptop by his employer.
48. On or around May 19, 2019, Pretrial Services Officer Patrick Kennedy conducted a routine home visit at DUNHAM's residence. Officer Kennedy found that DUNHAM was in possession of four prohibited devices – that being a PlayStation 3 gaming console and three flash drives. A court order was subsequently authorized permitting FBI agents to search the four devices. To-date, the three flash drives have been examined but the PlayStation 3 gaming console has not. Below is a summary of the results of the examination conducted to-date:
  - a. Approximately one image and approximately eleven videos of suspected child pornography were recovered from the deleted space of a Lexar-brand thumb drive. Also saved on the Lexar-brand thumb drive were images and videos depicting DUNHAM and/or his family members and approximately three documents with DUNHAM's name on them.
  - b. Approximately forty-eight images and approximately twenty-seven videos of suspected child pornography were recovered from the deleted space of a Crucial-brand thumb drive. Also recovered from both the active space and deleted space of the Crucial-brand thumb drive were more than one hundred and fifty images depicting Adult Female A and/or her three children. One of the images depicted one of Adult Female A's children, and it was photo-shopped or altered to depict the child nude and exposing her vagina. Furthermore, images depicting DUNHAM and/or his family members and approximately seven documents with DUNHAM's name on them were saved on the Crucial-brand thumb drive.
  - c. No child pornography files were recovered from the third thumb drive.
49. Officer Kennedy filed a Petition for Action on Conditions of Pretrial Release with the court regarding DUNHAM's possession of the four prohibited devices. A hearing was held regarding this petition on or around June 24, 2019. During the hearing, DUNHAM's bond was revoked. He was taken into custody by the United States Marshal's Service and is presently incarcerated at the Shelby County (Ohio) Jail.



50. On or around June 28, 2019 and July 8, 2019, I spoke to two representatives from DUNHAM's place of employment. The representatives provided the following information:
- a. DUNHAM was a Materials Planner for the company.
  - b. DUNHAM had not notified anyone from the company that he had been charged with child pornography offenses or that he was presently incarcerated. After DUNHAM's bond was revoked, one of DUNHAM's family members informed the company that DUNHAM could no longer report to work due to personal reasons. Company personnel conducted public records searches and learned of DUNHAM's arrest.
  - c. DUNHAM was issued the **SUBJECT DEVICE** as part of his employment. The **SUBJECT DEVICE** had access to the Internet, and DUNHAM was permitted to take it home with him. DUNHAM was the sole individual who used the **SUBJECT DEVICE**.
  - d. The **SUBJECT DEVICE** belonged to the company. All of the company's computer devices were subject to monitoring by company personnel at any time, and employees were informed of this on a regular basis.
51. Company representatives voluntarily turned over the **SUBJECT DEVICE** to me and provided their consent for the FBI to search it. The **SUBJECT DEVICE** was subsequently secured at the FBI's office located at 7747 Clys Road, Centerville, Ohio, and it has otherwise not been accessed.

Evidence Sought in Requested Search Warrant

52. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices in furtherance of their child pornography and child exploitation activities. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure. Based on this and other information detailed in the Affidavit, it is reasonable to believe that DUNHAM may have utilized the **SUBJECT DEVICE** in furtherance of his child pornography and child exploitation activities.
53. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

54. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chat rooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
55. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences and on their cellular telephones.
56. Based on all the information detailed in this Affidavit, I submit there is probable cause to believe that the **SUBJECT DEVICE** may contain evidence of DUNHAM's child pornography and child exploitation offenses.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

57. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.
58. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICE** may still be stored there, for at least the following reasons:
  - a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
  - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In



addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
  - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
59. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on **SUBJECT DEVICE** because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
  - b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
  - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

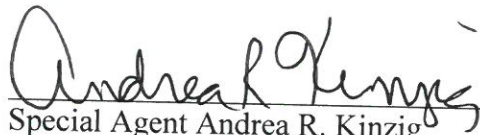
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

- 60. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.
- 61. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

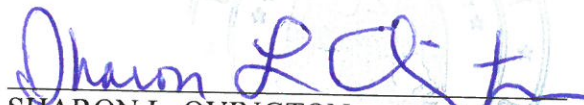


**CONCLUSION**

62. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; may be located on **SUBJECT DEVICE**, as described in Attachment A, in violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1)
63. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

  
Special Agent Andrea R. Kinzig  
Federal Bureau of Investigation

SUBSCRIBED and SWORN  
before me this 18<sup>th</sup> of July 2019

  
SHARON L. OVINGTON  
UNITED STATES MAGISTRATE JUDGE